US-CERT National Cyber Alert System

SB04-280-Summary of Security Items from September 29 through October 5, 2004

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Computer Associates Common Services 1.0, 1.1, 2.0, 2.1, 2.2, 3.0, Unicenter Network & Systems Management 3.0, Unicenter ServicePlus Service Desk 6.0	A vulnerability exists because the Server Admin password is stored in plaintext in certain installation batch files, which could let a malicious user obtain sensitive information. Patch and post installation steps available at: http://supportconnect.ca.com/sc/solcenter/sol_detail.jsp?aparno=QO58447&os=NT&returninput=0 There is no exploit code required.	Computer Associates Unicenter Common Services Plaintext Password	Medium	Secunia Advisory, SA12639, September 29, 2004
Kaspersky Lab KAV 5.0.149, 5.0.153	A vulnerability exists because RAMcleaner can be used to load the 'KAV.exe' application, which could let a malicious user bypass authentication. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Kaspersky Anti-Virus Authentication Bypass	Medium	SecurityTracker Alert ID, 1011479, October 1, 2004
Microsoft Internet Explorer 5.5, SP1&SP2. 6.0, SP1	A vulnerability exists due to insufficient validation of drag and drop events issued from the 'Internet' zone, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. **A Proof of Concept exploit script is reportedly being used by malicious Web sites to install Backdoor.Akak on victim computers.**	Internet Explorer Drag & Drop File Installation	High	Secunia Advisory, SA12321 August 19, 2004 **SecurityFocus, September 28, 2004**
Microsoft SQL Server 7.0 SP3 & prior	A remote Denial of Service vulnerability exists in 'mssqlserver' when a malicious user submits a large buffer that contains specially crafted data. No workaround or patch available at time of publishing. **Proofs of Concept exploit scripts have been published.**	Microsoft SQL Server Remote Denial of Service	Low	SecurityTracker Alert ID, 1011434, September 28, 2004 **SecurityFocus, September 30, 2004**
Microsoft Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional Server, SP-	A remote Denial of Service vulnerability exists in the Microsoft (Graphics Device Interface) GDI+ library when handling malformed JPEG files. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	Microsoft GDI+ Library Malformed JPEG Handling Remote Denial of Service	Low	Bugtraq, September 26, 2004

SP4, 2000 Server, SP1-SP4, Windows XP Home, SP1&SP2, XP Professional, SP1&SP2				
MyWebServer LLC MyWebServer 1.0.3	A remote Denial of Service vulnerability exists due to an error in the connection handling. No workaround or patch available at time of publishing. There is no exploit code required.	MyWebServer Remote Denial of Service	Low	Unl0ck Team Security Advisory, September 27, 2004
NetworkActiv NetworkActiv Web Server 1.0	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted HTTP GET request. Update available at: http://www.networkactiv.com/NetworkActivWebServerV1.0.exe A Proof of Concept exploit has been published.	NetworkActiv Web Server Remote Denial of Service	Low	Global Security Solution Advisory, October 5, 2004
Playlogic International Alpha Black Zero 1.0 4	A remote Denial of Service vulnerability exists due to insufficient restrictions on the total amount of connected clients. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Playlogic Alpha Black Zero Remote Denial of Service	Low	Bugtraq, September 29, 2004
Rebellion Judge Dredd: Dredd vs. Death 1.01 & prior	A format string vulnerability exists when handling a specially crafted chat message, which could let a remote malicious user cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Judge Dredd: Dredd vs. Death Format String	Low	Securiteam, October 4, 2004
RhinoSoft.com Serv-U 3.0, 3.1, 4.0 .0.4, 4.1 .0.11, 4.1, 4.2, 5.0 .0.9, 5.0 .0.6, 5.0.0.4, 5.1 .0, 5.2 .0.0	A remote Denial of Service vulnerability exists due to insufficient validation of arguments passed via the 'STOU' command. **Upgrade available at: http://www.serv-u.com/customer/record.asp?prod=su** There is no exploit code required; however, Proof of Concept exploit has been published.	Serv-U FTP Server Remote Denial of Service	Low	Bugtraq, September 11, 2004 **SecurityFocus, September 30, 2004**
Symantec Norton Antivirus 2003, 2004, 2005	A vulnerability exists because a file or directory name that contains certain character strings related to MS-DOS device names will not be scanned, which could let a remote malicious user execute arbitrary code. The vendor has issued a fix for Symantec Norton Anti-Virus 2004, available via LiveUpdate. We are not aware of any exploits for this vulnerability.	Symantec Norton Anti-Virus MS-DOS Name CVE Name: CAN-2004-0920	High	iDEFENSE Security Advisory, October 5, 2004
VyPRESS Messenger 3.5, 3.5.1	A buffer overflow vulnerability exists due to a boundary error in a visualization function, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.vypress.com/ftp/betas/VyMes40rc1.msi A Proof of Concept exploit script has been published.	VyPRESS Messenger Remote Buffer Overflow	High	Secunia Advisory, SA12605, October 1, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Aladdin Enterprises Ghostscript 4.3, 4.3.2, 5.10 cl, 5.10.10 -1 mdk, 5.10.10 -1, 5.10.10 mdk, 5.10.10, 5.10.12 cl, 5.10.15, 5.10.16, 5.50, 5.50.8 _7, 5.50.8, 6.51, 6.52, 6.53, 7.0 4-7.07	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	GhostScript Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
Apple MacOS X 10.3.5	Two vulnerabilities exist in the AFP Server; a Denial of Service vulnerability exists because a malicious user can mount an Apple File Protocol (AFP) volume and modify SessionDestroy packets; and a vulnerability exists in the AFP Drop Box due to an incorrect setting of the guest group id, which could let a remote malicious user obtain sensitive information. Updates available at: /http://www.apple.com/support/downloads/ We are not aware of any exploits for this vulnerability.	Apple AFP Server Mount Session Termination & Sensitive Information Disclosure CVE Names: CAN-2004-0921, CAN-2004-0922	Medium	Apple Security Update, APPLE-SA-2004-09-30, October 4, 2004
Apple MacOS X 10.2.8, 10.3.5	A vulnerability exists in NetInfo Manager because the account status for the 'root' user account may be displayed incorrectly, which could let a malicious user modify sensitive information. Update available at: http://www.apple.com/support/downloads/	NetInfo Manager Root Account Status Display CVE Name:	Medium	Apple Security Advisory, SA-2004-09-30, October 4, 2004

	We are not aware of any exploits for this vulnerability.	CAN-2004-0924		
Apple MacOS X 10.2.8, 10.3.5	A vulnerability exists in postfix when SMTPD AUTH has been enabled because the system does not properly clear a buffer containing the username after authentication attempts, which could let a remote malicious user prevent other users from authentication. Update available at: http://www.apple.com/support/downloads/ We are not aware of any exploits for this vulnerability.	Postfix Buffer Error Remote Authentication Prevention CVE Name: CAN-2004-0925	Medium	Apple Security Advisory, SA-2004-09-30, October 4, 2004
Apple MacOS X 10.2.8, 10.3.5	A vulnerability exists in ServerAdmin because the same common self-signed certificate is used if the administrator has not replaced this example certificate, which could let a remote malicious user obtain sensitive information. Update available at: http://www.apple.com/support/downloads/ We are not aware of any exploits for this vulnerability.	Apple ServerAdmin Default Certificate CVE Name: CAN-2004-0927	Medium	Apple Security Advisory, SA-2004-09-30, October 4, 2004
Apple MacOS X 10.2.8, 10.3.5	A buffer overflow vulnerability exists due to a boundary error within the handling of BMP images, which could let a remote malicious user execute arbitrary code. Update available at: http://www.apple.com/support/downloads/ We are not aware of any exploits for this vulnerability.	QuickTime Buffer Overflow CVE Name: CAN-2004-0926	High	Apple Security Advisory, SA-2004-09-30, October 4, 2004
Charles Cazabon getmail 4.0.0b10, 4.0-4.0.13, 4.1-4.1.5; Gentoo Linux 1.4	A vulnerability exists due to insufficient validation of symbolic links when creating users' mail boxes and subdirectories, which could let a malicious user obtain elevated privileges. Upgrades available at: http://www.qcc.ca/~charlesc/software/getmail-4/old-versions/getmail-4.2.0.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200409-32.xml **Debian: http://security.debian.org/pool/updates/main/g/getmail/** There is no exploit code required.	Getmail Privilege Escalation	Medium	Secunia Advisory, SA12594, September 20, 2004 **Debian Security Advisory, DSA 553-1, September 27, 2004**
Donald R Woods Spider 1.1	A buffer overflow vulnerability exists in 'movelog.c' due to a boundary error in the 'read_file()' function, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Spider Game Buffer Overflow	High	Secunia Advisory, SA12716, October 4, 2004
FreeBSD FreeBSD 5.x	A vulnerability exists in "CONS_SCRSHOT ioctl(2)' due to insufficient validation of user-supplied input, which could let a malicious user obtain sensitive information. Update available at: http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/dev/syscons/syscons.c#rev1.429 We are not aware of any exploits for this vulnerability.	FreeBSD syscons Input Validation CVE Name: CAN-2004-0919	Medium	SecurityTracker Alert ID, 1011526, October 4, 2004
FreeBSD/OpenBSD FreeBSD 4.6.2, 4.7-4.9, 5.0-5.2; OpenBSD 3.3, 3.4	A remote Denial of Service vulnerability exists due to the way out-of-sequence packets are handled. FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:04/tcp47.patch OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **SGI: http://www.sgi.com/support/security/** We are not aware of any exploits for this vulnerability.	BSD Out-of- Sequence Packets Remote Denial of Service CVE Name: CAN-2004-0171	Low	FreeBSD Security Advisory, FreeBSD-SA-04:04.tcp, March 2, 2004 **SGI Security Advisory, 20040905-01-P, September 28,2004**
GNU gettext 0.14.1	A vulnerability exists due to the insecure creation of temporary files, which could possible let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	GNU GetText Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
GNU glibc 2.0-2.0.6, 2.1, 2.1.1 -6, 2.1.1, 2.1.2, 2.1.3 -10, 2.1.3, 2.1.9 & greater, 2.2-2.2.5, 2.3-2.3.4, 2.3.10	A vulnerability exists due to the insecure creation of temporary files, which could possible let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	GNU GLibC Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
GNU groff 1.19	A vulnerability exists due to the insecure creation of temporary files, which could possible let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	GNU Troff (Groff) Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
GNU gzip 1.2.4 a	A vulnerability exists due to the insecure creation of temporary files, which could possible let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/	GNU GZip Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050,

	There is no exploit code required.			September 30, 2004
GNU sharutils 4.2, 4.2.1	Multiple buffer overflow vulnerabilities exists due to a failure to verify the length of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200410-01.xml We are not aware of any exploits for this vulnerability.	GNU Sharutils Multiple Buffer Overflow	Low/High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200410-01, October 1, 2004
IBM AIX 5L Version 5.2 on pSeries, 5.3 on pSeries, 5.2, 5.3 on an i5/OS (iSeries) partition, Tivoli System Automation (TSA) for Linux 1.1, Multiplatforms 1.2, Cluster Systems Management (CSM) for Linux Version 1.4, (version 1.4 and greater), Hardware Management Console (HMC) for pSeries Version 3, , General Parallel File System (GPFS) Version 2 Release 2 on Linux for xSeries and Linux for pSeries	An input validation vulnerability exists in the Reliable Scalable Cluster Technology (RSCT) system 'ctstrtcasd,' which could let a malicious user create or corrupt arbitrary files. **Updates and workaround available at: http://techsupport.services.ibm.com/** A Proof of Concept exploit has been published.	IBM Reliable Scalable Cluster Technology (RSCT) File Corruption CVE Name: CAN-2004-0828	Medium	iDEFENSE Security Advisory, September 27, 2004 **SecurityFocus, September 29, 2004**
Larry Wall Perl 5.8.3	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	Perl Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
LBL Debian Mandrake OpenPKG Trustix SGI Slackware tcpdump 3.4 a6, 3.4, 3.5 alpha, 3.5, 3.5.2, 3.6.2 3.6.3, 3.7-3.7.2, 3.8.1	Two vulnerabilities exist: a buffer overflow vulnerability exists in 'print-isakmp.c' due to insufficient validation of user-supplied input in ISAKMP packets, which could let a remote malicious user cause a Denial of Service and possibly allow the execution of arbitrary code; and a vulnerability exists when a remote malicious user submits an ISAKMP Identification payload with a specially crafted payload length value that is less than eight bytes. Upgrades available at: http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/t/tcpdump Mandrake: Http://www.mandrakesecure.net/en/advisories/ OpenPKG: ftp://ftp.openpkg.org/release/ Slackware: ftp://ftp.slackware.com/pub/slackware/ SGI: http://www.sgi.com/support/security/ **Fedora Legacy: http://download.fedoralegacy.org/redhat/** An exploit script has been published for the ISAKMP Identification Payload vulnerability	TCPDump ISAKMP Buffer Overflow & ISAKMP Identification Payload Integer Underflow CVE Names: CAN-2004-0183, CAN-2004-0184	Low/High (High if arbitrary code can be executed)	Debian Security Advisory, DSA 478-1, April 6, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:030, April 15, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.010, April 7, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0015, March 30, 2004 SGI Security Advisories, 20040602-01-U & 20040603-01-U, June 21, 2004 Slackware Security Advisory, SSA:2004-108-01, April 17, 2004 **Fedora Legacy Update Advisory, FLSA:1468, September 29, 2004**
Martin Pool distcc prior to 2.16	A vulnerability exists because access controls are not properly enforced, which could let a malicious user bypass certain security restrictions. Updates available at: http://distcc.samba.org/download.html We are not aware of any exploits for this vulnerability.	distcc Address Parsing CVE Name: CAN-2004-0601	Medium	Secunia Advisory, SA12711, October 4, 2004
MediaWiki MediaWiki 1.3-1.3.4	A Cross-Site Scripting vulnerability exists due to an input validation error in the 'raw' page output mode, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/wikipedia/	MediaWiki Raw Page Cross-Site Scripting	High	Secunia Advisory, SA12692, October 1, 2004

	mediawiki-1.3.5.tar.gz?download There is no exploit code required.			
MIT Kerberos 5 1.3.4	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	MIT Kerberos 5 Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
Multiple Vendors ArX Distributed Revision Control System 1.0 pre10-pre16, 1.0.17, 1.0.18; Cadaver WebDAV Client 0.20 .0- 0.20.5, 0.21 .0, 0.22.0; Neon Client Library 0.19.3, 0.23- 0.23.8, 0.24- 0.24.4; Netwosix Netwosix Linux 1.0, 1.1; RedHat Advanced Work-station for the Itanium Processor 2.1, Enterprise Linux WS 2.1, ES 2.1, AS 2.1	Multiple format string vulnerabilities exist when processing XML/207 response messages, which could let a remote malicious user execute arbitrary code. ArX Distributed: http://superbeast.ucsd.edu/~landry/ArX/ArX-1.0.19.tar.gz Cadaver: http://www.webdav.org/cadaver/ Debian: http://security.debian.org/pool/updates/main/n/neon/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Neon Client: http://www.webdav.org/neon/neon-0.24.5.tar.gz Netwosix: http://download.netwosix.org/0012/nepote OpenPKG: ftp.openpkg.org/release/2.0/UPD/neon-0.24.4-2.0.1.src.rpm RedHat: ftp://updates.redhat.com/9/en/os/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ SuSE: ftp://ftp.suse.com/pub/suse/i386/update **Fedora Legacy: http://download.fedoralegacy.org/redhat/** An exploit has been published.	WebDAV Client Library Format String Vulnerabilities CAN-2004-0179	High	Red Hat Security Advisories, RHSA-2004: 157-06, 158-01, & 159-01, April 14 & 15, 2004 Debian Security Advisory, DSA 487-1, April 16, 2004 SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.016, April 16, 2004 Netwosix Linux Security Advisory #2004-0012, April 18, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:032, April 20, 2004 SGI Security Advisory, 20040404-01-U, April 21, 2004 **Fedora Legacy Update Advisory, FLSA:1552, September 29, 2004**
Multiple Vendors Cisco VPN 3000 Concentrator 4.0 .x, 4.0, 4.0.1, 4.1 .x; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux 1.4 _rc1-rc3, 1.4; MandrakeSoft Corporate Server 2.1, x86_64, Linux Mandrake 9.1, ppc, 9.2, amd64, 10.0, AMD64, MandrakeSoft Multi Network Firewall 8.2; MIT Kerberos 5 1.0, 1.0.6, 1.0.8, 1.1, 1.1.1, 1.2-1.2.8, 1.3 -1.3.4; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3, Fedora Core2, Core1; Sun SEAM 1.0.2	Multiple double-free vulnerabilities exist due to inconsistent memory handling routines in the krb5 library: various double-free errors exist in the KDC (Key Distribution Center) cleanup code and in client libraries, which could let a remote malicious user execute arbitrary code; various double-free errors exist in the 'krb5_rd_cred()' function, which could let a remote malicious user execute arbitrary code; a double-free vulnerability exists in krb524d, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in ASN.1 decoder when handling indefinite length BER encodings, which could let a remote malicious user cause a Denial of Service. MIT Kerberos: http://web.mit.edu/kerberos/advisories/ Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-09.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-21-112908-15-1 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000860 OpenPKG: ftp://ftp.openpkg.org/release/	Kerberos 5 Double-Free Vulnerabilities CVE Names: CAN-2004-0642, CAN-2004-0643, CAN-2004-0772	Low/High (High if arbitrary code can be executed)	MIT krb5 Security Advisory, MITKRB5-SA-2004-002, August 31, 2004 US-CERT Technical Cyber Security Alert TA04-247A, September 5, 2004 US-CERT Vulnerability Notes, VU#350792, VU#795632, VU#866472, September 3, 2004 Conectiva Security Advisory, CLSA-2004:860, September 9, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.039, September 13,

	TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Server/ **IBM: http://www.securityfocus.com/advisories/7269** We are not aware of any exploits for this vulnerability.			2004 Turbolinux Security Advisory TLSA-2004-22, September 15, 2004 **IBM Security Advisory, September 30, 2004**
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; GNU Emacs 20.0-20.6, 21.2	A vulnerability exists in the Emacs film library due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/f/flim/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-344.html **Fedora Legacy: http://download.fedoralegacy.org/redhat/** We are not aware of any exploits for this vulnerability.	Emacs film Library Insecure Temporary File Creation CVE Name: CAN-2004-0422	Medium	Debian Security Advisory, DSA 500-1, May 2, 2004 **Fedora Legacy Update Advisory, FLSA:1581, September 30, 2004**
Multiple Vendors Debian Mandrake OpenPKG RedHat SGI Slackware Trustix Debian Linux 3.0, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; rsync 2.3.1, 2.3.2 -1.3, 2.3.2 -1.2, sparc, PPC, m68k, intel, ARM, alpha, 2.3.2, 2.4.0, 2.4.1, 2.4.3- 2.4.6, 2.4.8, 2.5.0- 2.5.7, 2.6	A vulnerability exists due to insufficient sanitization of user-supplied path values, which could let a remote malicious user modify system information or obtain unauthorized access. Debian: http://security.debian.org/pool/updates/main/r/rsync Mandrake: http://www.mandrakesecure.net/en/ftp.php Rsync: http://rsync.samba.org/ftp/rsync/rsync-2.6.1.tar.gz Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://www.trustix.org/errata/misc/2004/TSL-2004-0024-rsync.asc.txt OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-192.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/ Apple: http://www.apple.com/support/security/security_updates.html **Fedora Legacy: http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	RSync Path Validation CVE Name: CAN-2004-0426	Medium	Debian Security Advisory, DSA 499-1, May 2, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:042, May 11, 2004 OpenPKG Security Advisory , OpenPKG-SA-2004.025, May 21, 2004 RedHat Security Advisory, RHSA-2004:192-06, May 19, 2004 SGI Security Advisories, 20040508-01-U & 20040509-01, May 28, 2004 Slackware Security Advisory, SSA:2004-124-01, May 3, 2004 Trustix Secure Linux Security Advisory, 2004-0024, April 30, 2004 **Fedora Legacy Update Advisory, FLSA:2003, September 30, 2004**
Multiple Vendors Easy Software Products CUPS 1.1.14-1.1.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A Denial of Service vulnerability exists in 'scheduler/dirsvc.c' due to insufficient validation of UDP datagrams. Update available at: http://www.cups.org/software.php Debian: http://security.debian.org/pool/updates/main/c/cupsys/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ ALTLinux: http://altlinux.com/index.php?module=sisyphus&package=cups Gentoo: http://security.gentoo.org/glsa/glsa-200409-25.xml Slackware: ftp://ftp.slackware.com/pub/slackware/	CUPS Browsing Denial of Service CVE Name: CAN-2004-0558	Low	SecurityTracker Alert ID, 1011283, September 15, 2004 ALTLinux Advisory, September 17, 2004 Gentoo Linux Security Advisory GLSA 200409-25, September 20, 2004 Slackware Security Advisory, SSA:2004-266-01, September 23, 2004

	Apple: http://www.apple.com/support/security/security_updates.html **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** A Proof of Concept exploit has been published.			**Fedora Update Notification, FEDORA-2004-275, September 28, 2004** **Apple Security Update, APPLE-SA-2004-09-30, October 4, 2004**
Multiple Vendors FileZilla Server 0.7, 0.7.1; OpenBSD -current, 3.5; OpenPKG Current, 2.0, 2.1; zlib 1.2.1	A remote Denial of Service vulnerability during the decompression process due to a failure to handle malformed input. Gentoo: http://security.gentoo.org/glsa/glsa-200408-26.xml FileZilla: http://sourceforge.net/project/showfiles.php?group_id=21558 OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/017_libz.patch OpenPKG: ftp ftp.openpkg.org Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ SuSE: ftp://ftp.suse.com/pub/suse/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ We are not aware of any exploits for this vulnerability.	Zlib Compression Library Remote Denial of Service CVE Name: CAN-2004-0797	Low	SecurityFocus, August 25, 2004 SUSE Security Announcement, SUSE-SA:2004:029, September 2, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:090, September 8, 2004 Conectiva Linux Security Announcement, CLA-2004:865, September 13, 2004 **US-CERT Vulnerability Note VU#238678, October 1, 2004**
Multiple Vendors GNU Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; GNOME gdk-pixbug 0.22 & prior; GTK GTK+ 2.0.2, 2.0.6, 2.2.1, 2.2.3, 2.2.4; MandrakeSoft Linux Mandrake 9.2, amd64, 10.0, AMD64; RedHat Advanced Workstation for the Itanium Processor 2.1, IA64, Desktop 3.0, Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, ES 2.1 IA64, ES 2.1, AS 3, AS 2.1 IA64, AS 2.1, RedHat Fedora Core1&2; SuSE. Linux 8.1, 8.2, 9.0, x86_64, 9.1, Desktop 1.0, Enterprise Server 9, 8	Multiple vulnerabilities exist: a vulnerability exists when decoding BMP images, which could let a remote malicious user cause a Denial of Service; a vulnerability exists when decoding XPM images, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a vulnerability exists when attempting to decode ICO images, which could let a remote malicious user cause a Denial of Service. Debian: http://security.debian.org/pool/updates/main/g/gdk-pixbuf/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SuSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-28.xml We are not aware of any exploits for this vulnerability.	gdk-pixbug BMP, ICO, and XPM Image Processing Errors CVE Names: CAN-2004-0753, CAN-2004-0782, CAN-2004-0783, CAN-2004-0788	Low/High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011285, September 17, 2004 Gentoo Linux Security Advisory, GLSA 200409-28, September 21, 2004 **US-CERT Vulnerability Notes VU#577654, VU#369358, VU#729894, VU#825374, October 1, 2004**
Multiple Vendors OpenBSD 3.4, 3.5; SuSE Linux 8.1, 8.2, 9.0, x86_64, 9.1, Linux Enterprise Server 9, 8; X.org X11R6 6.7.0, 6.8; XFree86 X11R6 3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1, Errata, 4.3.0	Multiple vulnerabilities exist: a stack overflow exists in 'xpmParseColors()' in 'parse.c' when a specially crafted XPMv1 and XPMv2/3 file is submitted, which could let a remote malicious user execute arbitrary code; a stack overflow vulnerability exists in the 'ParseAndPutPixels()' function in -create.c' when reading pixel values, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists in the colorTable allocation in 'xpmParseColors()' in 'parse.c,' which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenBSD: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/ SuSE: ftp://ftp.suse.com/pub/suse/ X.org: http://x.org/X11R6.8.1/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-34.xml** **IBM: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp** **RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html**	LibXpm Image Decoding Multiple Remote Buffer Overflow CVE Names: CAN-2004-0687, CAN-2004-0688	High	X.Org Foundation Security Advisory, September 16, 2004 **US-CERT Vulnerability Notes, VU#537878 & VU#882750, September 30, 2004** **SecurityFocus, October 4, 2004**

	Proofs of Concept exploits have been published.			
Multiple Vendors Samba Samba 2.2 a, 2.2 .0a, 2.2 .0, 2.2.1 a, 2.2.2, 2.2.3 a, 2.2.3-2.2.9, 2.2.11, 3.0, alpha, 3.0.1-3.0.5; MandrakeSoft Corporate Server 2.1, x86_64, 9.2, amd64	A vulnerability exists due to input validation errors in 'unix_convert()' and 'check_name()' when converting DOS path names to path names in the internal filesystem, which could let a remote malicious user obtain sensitive information. Samba: http://download.samba.org/samba/ftp/patches/security/ http://us1.samba.org/samba/ftp/old-versions/samba-2.2.12.tar.gz Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	Samba Remote Arbitrary File Access CVE Name: CAN-2004-0815	Medium	iDEFENSE Security Advisory, September 30, 2004
MySQL AB MySQL 4.0.18	A vulnerability exists due to the insecure creation of temporary files, which could possible let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	MySQL Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
Netatalk Netatalk Open Source Apple File Share Protocol Suite 1.5 pre6, 1.6.1, 1.6.4	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	NetaTalk Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
OpenOffice OpenOffice 1.1.2, Sun StarOffice 7.0	A vulnerability exists in the '/tmp' folder due to insecure permissions, which could let a malicious user obtain sensitive information. Upgrades available at: http://sunsolve.sun.com/search/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-446.html **Mandrake: http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.	OpenOffice/ StarOffice Insure Temporary File Permissions CVE Name: CAN-2004-0752	Medium	Secunia Advisory, SA12302, September 13, 2004 RedHat Security Bulletin, RHSA-2004:446-08, September 15, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:103, September 28, 2004**
OpenSSL Project OpenSSL 0.9.6, 0.9.6 a-0.9.6 m, 0.9.7c	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	OpenSSL Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
Peter Zelezny X-Chat 1.8-1.8.2, 1.8.6-1.8.9, 2.0.1, 2.0.5- 2.0.8	A buffer overflow vulnerability exists in the SOCKS 5 proxy code, which could let a remote malicious user execute arbitrary code. Patch available at: http://www.xchat.org/files/source/2.0/patches/xc208-fixsocks5.diff Debian: http://security.debian.org/pool/updates/main/x/xchat/ Gentoo:http://security.gentoo.org/glsa/glsa-200404-15.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Netwosix: http://www.netwosix.org/adv14.html RedHat: ftp://updates.redhat.com/9/en/os/ **Fedora Legacy: http://download.fedoralegacy.org/redhat/** An exploit script has been published.	XChat SOCKS 5 Remote Buffer Overflow CVE Name: CAN-2004-0409	High	Debian Security Advisory, DSA 493-1, April 21, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:036, April 22, 2004 Red Hat Security Advisory, RHSA-2004:177-01, April 30, 2004 Netwosix Linux Security Advisory, LNSA-#2004-0014, May 1, 2004 Packet storm, May 4, 2004 **Fedora Legacy Update Advisory, FLSA:1549, September 30, 2004**
PostgreSQL PostgreSQL 7.4.5	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	PostgreSQL Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004

Roaring Penguin Software Roaring Penguin 3.5 & prior	A vulnerability exists in the pppoe driver, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/r/rp-pppoe/ We are not aware of any exploits for this vulnerability.	Roaring Penguin pppoe Elevated Privileges CVE Name: CAN-2004-0564	Medium	Debian Security Advisory, DSA 557-1 , October 4, 2004
rsync 2.6.2 and prior Debian SuSE Trustix	A vulnerability exists in rsync when running in daemon mode with chroot disabled. A remote user may be able read or write files on the target system that are located outside of the module's path. A remote user can supply a specially crafted path to cause the path cleaning function to generate an absolute filename instead of a relative one. The flaw resides in the sanitize_path() function. Updates and patches are available at: http://rsync.samba.org/ SuSE: http://www.suse.de/de/security/2004_26_rsync.html Debian: http://www.debian.org/security/2004/dsa-538 Trustix: http://www.trustix.net/errata/2004/0042/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/2.0/UPD/ Tinysofa: http://http.tinysofa.org/pub/tinysofa/updates/server-2.0/i386/tinysofa/rpms.updates/rsync-2.6.2-2ts.i386.rpm TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ **Fedora Legacy: http://download.fedoralegacy.org/redhat/** We are not aware of any exploits for this vulnerability.	Rsync Input Validation Error in sanitize_path() May Let Remote Users Read or Write Arbitrary Files CVE Name: CAN-2004-0792	High	SecurityTracker 1010940, August 12, 2004 rsync August 2004 Security Advisory SecurityFocus, September 1, 2004 **Fedora Legacy Update Advisory, FLSA:2003, September 30, 2004**
SGI IRIX 6.5.22-6.5.25	A vulnerability exists because 't_unbind()' modifies the expected behavior of 't_bind().' The consequences of the vulnerability are not known. Patches available at: ftp://patches.sgi.com/support/free/security/patches/ We are not aware of any exploits for this vulnerability.	SGI 'bsd.a' Kernel Networking Flaw CVE Name: CAN-2004-0139	Not Specified	SGI Security Advisory, September 28, 20040905-01-P, 2004
SpamAssassin.org SpamAssassin prior to 2.64	A Denial of Service vulnerability exists in SpamAssassin. A a remote user can send an e-mail message with specially crafted headers to cause a Denial of Service attack against the SpamAssassin service. Update to version (2.64), available at: http://old.spamassassin.org/released/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **RedHat: http://rhn.redhat.com/errata/RHSA-2004-451.html** We are not aware of any exploits for this vulnerability.	SpamAssassin Remote Denial of Service CVE Name: CAN-2004-0796	Low	SecurityTracker: 1010903, August 10, 2004 Mandrake Security Advisory, MDKSA-2004:084, August 19, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.041, September 15, 2004 Conectiva Linux Security Announcement, CLA-2004:867, September 22, 2004 **RedHat Security Advisory, RHSA-2004:451-05, September 30, 2004**
Squid-cache.org Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.4, STABLE7, 2.5 STABLE1-STABLE6, Squid Web Proxy Cache 3.0 PRE1-PRE3	A remote Denial of Service vulnerability exists in 'lib/ntlmauth.c' due to insufficient validation of negative values in the 'ntlm_fetch_string()' function. Patches available at: http://www1.uk.squid-cache.org/squid/Versions/v2/2.5/bugs/squid-2.5.STABLE6-ntlm_fetch_string.patch Gentoo: http://security.gentoo.org/glsa/glsa-200409-04.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ **RedHat: http://rhn.redhat.com/errata/RHSA-2004-462.html** **TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/**	Squid Proxy NTLM Authentication Remote Denial of Service CVE Name: CAN-2004-0832	Low	Secunia Advisory, SA12444, September 3, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:093, September 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0047, September 16,

	We are not aware of any exploits for this vulnerability.			2004 **RedHat Security Advisory, RHSA-2004:462-10, September 30, 2004** **\Turbolinux Security Announcement, October 5, 2004**
Subversion Subversion 1.0-1.0.7, 1.1 .0 rc1-rc3	A vulnerability exists in the 'mod_authz_svn' module due to insufficient restricted access to metadata on unreadable paths, which could let a remote malicious user obtain sensitive information. Update available at: http://subversion.tigris.org/tarballs/subversion-1.0.8.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ **Gentoo: http://security.gentoo.org/glsa/glsa-200409-35.xml** There is no exploit code required.	Subversion Mod_Authz_Svn Metadata Information Disclosure CVE Name: CAN-2004-0749	Medium	SecurityTracker Alert ID, 1011390, September 23, 2004 **Gentoo Linux Security Advisory, GLSA 200409-35, September 29, 2004**
Sun Microsystems, Inc. Solaris 8	A vulnerability exists in the gzip(1) command, which could let a malicious user access the files of other users that were processed using gzip. Workaround and update available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57600-1 We are not aware of any exploits for this vulnerability.	Sun Solaris Gzip File Access	Medium	Sun(sm) Alert Notification, 57600, October 1, 2004
Trustix LVM Logical Volume Management Utilities 1.0.7	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ There is no exploit code required.	Trustix LVM Utilities Insecure Temporary File Creation	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004
Viagenie Freenet6 0.9.6, 1.0	A vulnerability exists because the 'tspc.conf' configuration file for the freenet6 client is world-readable, which could let a malicious user obtain sensitive information. Debian: http://security.debian.org/pool/updates/main/f/freenet6/ There is no exploit code required.	Freenet6 on Debian Linux Information Disclosure CVE Name: CAN-2004-0563	Medium	Debian Security Advisory DSA 555-1, September 30, 2004
xmlstar.sourceforge.net XMLStartlet prior to 0.9.5	Several buffer overflow vulnerabilities exist when processing XML data in 'xml_elem.c' and 'xml_select.c,' which could let a remote malicious user execute arbitrary code. Numerous format string vulnerabilities also exist when processing useage parameters, which could let a remote malicious user execute arbitrary code. Update available at: http://xmlstar.sourceforge.net/download.php We are not aware of any exploits for this vulnerability.	XMLStartlet Buffer Overflows & Format Strings	High	SecurityTracker Alert ID, 1011496, October 1, 2004
Yukihiro Matsumoto Ruby 1.6, 1.8	A vulnerability exists in the CGI session management component due to the way temporary files are processed, which could let a malicious user obtain elevated privileges. Upgrades available at: http://security.debian.org/pool/updates/main/r/ruby/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-08.xml **RedHat: http://rhn.redhat.com/errata/RHSA-2004-441.html** We are not aware of any exploits for this vulnerability.	Ruby CGI Session Management Unsafe Temporary File CVE Name: CAN-2004-0755	Medium	Debian Security Advisory, DSA 537-1, August 16, 2004 Gentoo Linux Security Advisory, GLSA 200409-08, September 3, 2004 **RedHat Security Advisory, RHSA-2004:441-18, September 30, 2004**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
@lexPHPteam @lex Guestbook	An input validation vulnerability exists in @lex Guestbook, which could let a remote malicious user execute arbitrary PHP code. **Update available at: http://www.alexphpteam.com/download.php** We are not aware of any exploits for this vulnerability.	@lex Guestbook Include File Remote Code Execution	High	SecurityTracker Alert ID, 1011432, September 28, 2004 **SecurityFocus, September 30, 2004**
Apache Software	A remote Denial of Service vulnerability exists due to a failure to properly	Xerces C++	Low	Bugtraq, October 2, 2004

Foundation Xerces C++ 2.5 .0	handle exceptional XML input. Upgrade available at: http://www.apache.org/dist/xml/xerces-c/xerces-c-src_2_6_0.tar.gz There is no exploit code required.	XML Parsing Remote Denial of Service		
bblog.com bBlog 0.7.2, bBlog 0.7.3	An input validation vulnerability exists in 'rss.php' due to insufficient sanitization of the 'p' array parameter, which could let a remote malicious user execute arbitrary SQL commands. Updates available at: http://www.bblog.com/download.php There is no exploit code required.	BBlog RSS.PHP Input Validation	High	Bugtraq, October 1, 2004
Fritz Berger yappa-ng prior to 2.3.0	Two vulnerabilities exists: a vulnerability exists in 'show.php' due to a security flaw when showing a random image, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when a malicious user requests that an image be resized to a large value. Updates available at: http://sourceforge.net/project/showfiles.php?group_id=70802 We are not aware of any exploits for this vulnerability.	yappa-ng Access Control	Low/ Medium (Medium if sensitive information can be obtained)	Secunia Advisory, SA12709, October 4, 2004
FuzzyMonkey.org My Blog prior to 1.21	Several vulnerabilities exist due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://www.fuzzymonkey.org/cgi-bin/newfuzzy/software.cgi We are not aware of any exploits for this vulnerability.	My Blog Input Validation Errors	High	Secunia Advisory, SA12729, October 5, 2004
Hewlett Packard Company LaserJet 4200, 4300	A vulnerability exists due to the method of upgrading the firmware on affected devices, which could let a remote malicious user cause a Denial of Service, replace the firmware with malicious code, or possibly render the printer useless until the firmware is repaired or replaced. No workaround or patch available at time of publishing. We are not aware of any exploits for this vulnerability.	HP LaserJet 4200/4300 Printer Arbitrary Firmware Upgrade	Low/High (High if arbitrary code can be executed)	SecurityFocus, September 30, 2004
Icecast.org Icecast 2.0, 2.0.1	A buffer overflow vulnerability exists due to a boundary error in the parsing of HTTP headers, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://svn.xiph.org/releases/icecast/icecast-2.0.2.tar.gz A Proof of Concept exploit script has been published.	Icecast Server HTTP Header Buffer Overflow	High	SecurityTracker Alert ID. 1011439, September 29, 2004
Macromedia ColdFusion MX 6.1	A vulnerability exists because remote authenticated malicious users with privileges to create templates that contain CreateObject and cfobject tags can create a template to access the administrative password. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ColdFusion MX Template Information Disclosure	Medium	SecurityTracker Alert ID, 1011475, October 1, 2004
Marc Druilhe W-Agora 4.1.6 a	Multiple vulnerabilities exist: a vulnerability exists in 'redir_url.php' due to insufficient sanitization of the 'key' parameter, which could let a remote malicious user execute arbitrary SQL code; a vulnerability exists due to insufficient sanitization of the 'thread' parameter in 'download_thread.php' and 'subscribe_threat.php' the 'loginuser' parameter in 'login.php,' and the 'userid' parameter in 'forgot_password.php,' which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in 'list.php,' which could let a remote malicious user obtain sensitive information. The vendor has issued a fix, available via CVS. There is no exploit code required; however, Proofs of Concept exploits have been published.	W-Agora Multiple Remote Input Validation Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1011463, September 30, 2004
Mozilla.org Firefox Preview Release, 0.8, 0.9 rc, 0.9-0.9.3, 0.10	A vulnerability exists due to an error when downloading files, which could let a remote malicious user delete files. susceptible to a file deletion vulnerability. Upgrades available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/0.10.1/firefox-1.0PR-source.tar.bz2 Patches available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/0.10.1/patches/259708.xpi There is no exploit code required.	Mozilla Firefox Save Dialog File Deletion	Medium	Secunia Advisory, SA12708, October 4, 2004
Mozilla.org Mandrakesoft Slackware Mozilla 1.7 and prior; Firefox 0.9 and prior;	Multiple vulnerabilities exist in Mozilla, Firefox, and Thunderbird that could allow a malicious user to conduct spoofing attacks, compromise a vulnerable system, or cause a Denial of Service. These vulnerabilities include buffer overflow, input verification, insecure certificate name matching, and out-of-bounds reads.	Mozilla Multiple Vulnerabilities CVE Name: CAN-2004-	High	Secunia, SA10856, August 4, 2004 US-CERT Vulnerability Note VU#561022

Thunderbird 0.7 and prior	Upgrade to the latest version of Mozilla, Firefox, or Thunderbird available at: http://www.mozilla.org/download.html Slackware: http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.667659 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:082 RedHat: http://rhn.redhat.com/errata/RHSA-2004-421.html SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-26.xml **HP: http://h30097.www3.hp.com/internet/download.htm** We are not aware of any exploits for this vulnerability.	0757, CAN-2004-0759, CAN-2004-0761 CAN-2004-0765		RedHat Security Advisory, RHSA-2004:421-17, August 4, 2004 SGI Security Advisory, 20040802-01-U, August 14, 2004 Gentoo Linux Security Advisory, GLSA 200409-26, September 20, 2004 **HP Security Bulletin, HPSBTU01081, October 5, 2004**
Mozilla.org Mozilla 0.x, 1.0-1.7.x, Firefox 0.x, Thunderbird 0.x; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2	Multiple vulnerabilities exist: buffer overflow vulnerabilities exist in 'nsMsgCompUtils.cpp' when a specially crafted e-mail is forwarded, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient restrictions on script generated events, which could let a remote malicious user obtain sensitive information; a buffer overflow vulnerability exists in the 'nsVCardObj.cpp' file due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'nsPop3Protocol.cpp' due to boundary errors, which could let a remote malicious user execute arbitrary code; a heap overflow vulnerability exists when handling non-ASCII characters in URLs, which could let a remote malicious user execute arbitrary code; multiple integer overflow vulnerabilities exist in the image parsing routines due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code; a cross-domain scripting vulnerability exists because URI links dragged from one browser window and dropped into another browser window will bypass same-origin policy security checks, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because unsafe scripting operations are permitted, which could let a remote malicious user manipulate information displayed in the security dialog. Updates available at: http://www.mozilla.org/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-26.xml **HP: http://h30097.www3.hp.com/internet/download.htm** **RedHat: http://rhn.redhat.com/errata/RHSA-2004-486.html** Proofs of Concept exploits have been published.	Mozilla Multiple Remote Vulnerabilities CVE Names: CAN-2004-0902, CAN-2004-0903, CAN-2004-0904, CAN-2004-0905, CAN-2004-0908	Medium/ High (High if arbitrary code can be executed)	Technical Cyber Security Alert TA04-261A, September 17, 2004 US-CERT Vulnerability Notes VU#414240, VU#847200, VU#808216, VU#125776, VU#327560, VU#651928, VU#460528, VU#113192, September 17, 2004 Gentoo Linux Security Advisory, GLSA 200409-26, September 20, 2004 **RedHat Security Bulletin, RHSA-2004:486-18, September 30, 2004** **HP Security Bulletin, HPSBTU01081, October 5, 2004**
Multiple Vendors AJ-Fork AJ-Fork 16-; CutePHP CuteNews 0.88, 1.3-1.3.2, 1.3.6	A vulnerability exists due to insecure default file permissions, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	AJ-Fork Insecure Default Permissions	Medium	Bugtraq, October 1, 2004.
Multiple Vendors Linux kernel 2.4.0-test1-test12, 2.4.1-2.4.27; Microsoft Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, XP Home, SP1&SP2, XP Professional, SP1&SP2	A remote Denial of Service vulnerability exists due to inefficiencies when handling fragmented TCP packets. No workaround or patch available at time of publishing. Exploit scripts have been published.	Multiple Vendor TCP Packet Fragmentation Handling Denial of Service	Low	Bugtraq, September 27, 2004
Multiple Vendors Multiple (See advisory located at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm for complete list)	A vulnerability exists that affects implementations of the Transmission Control Protocol (TCP) that comply with the Internet Engineering Task Force's (IETF's) Requests For Comments (RFCs) for TCP. The impact of this vulnerability varies by vendor and application but could let a remote malicious user cause a Denial of Service, or allow unauthorized malicious users to inject malicious data into TCP streams. List of updates available at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm **SGI: http://www.sgi.com/support/security/** Proofs of Concept exploits have been published. Vulnerability has appeared in the press and other public media.	Multiple Vendor TCP Sequence Number Approximation CVE Name: CAN-2004-0230	Low/High (High if arbitrary code can be executed)	NISCC Vulnerability Advisory, 236929, April 23, 2004 VU#415294, http://www.kb.cert.org/vuls/id/415294 TA04-111A, http://www.us-cert.gov/cas/techalerts/TA04-111A.html **SGI Security Advisory, 20040905-01-P, September 28,2004**
MySQL AB MySQL 4.1.3 -beta, 4.1.4	A buffer overflow vulnerability exists due to a failure to ensure the size of a buffer is sufficient to handle user-supplied input, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	MySQL Bounded Parameter Statement	Low/High (High if arbitrary	SecurityFocus, September 27, 2004

	Upgrades available at: http://dev.mysql.com/get/Downloads/MySQL-4.1/mysql-4.1.5-gamma.tar.gz/from/pick We are not aware of any exploits for this vulnerability.	Execution Remote Buffer Overflow	code can be executed)	
ParaChat Group ParaChat Server 5.5	A Directory Traversal vulnerability exists due to an input validation error, which could let a remote malicious user obtain sensitive information. The vendor has fixed the vulnerability in the latest version 5.5 without changing the version number. Update to a version released on 2004-09-29 or later. There is no exploit code required; however, a Proof of Concept exploit has been published.	ParaChat Server Directory Traversal	Medium	Secunia Advisory, SA12678, September 30, 2004
PHP-Fusion PHP-Fusion 4.0 1	Multiple vulnerabilities exist: a vulnerability exists due to insufficient sanitization of input passed to the 'rowstart' parameter in 'members.php' and the 'comment_id' parameter in 'comments.php,' which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists due to insufficient sanitization of input passed to fields in 'Submit News,' 'Submit Link,' and 'Submit Article,' which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	PHP-Fusion Multiple SQL & HTML Injection	High	Secunia Advisory, SA12686, September 30, 2004
phplinks.sourceforge.net PHPLinks	A vulnerability exists when a certain type of URL is requested, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PHPLinks Installation Path Disclosure	Medium	Nkxtox Advisory 0000-00003, October 3, 2004
proxytunnel proxytunnel 1.0.6, 1.1.3	A vulnerability exists because proxyuser/proxypass data is passed to the program in an insecure manner, which could let a malicious user obtain sensitive information. Upgrades available at: http://prdownloads.sourceforge.net/proxytunnel/proxytunnel-1.2.0.tgz?download There is no exploit code required.	Proxytunnel Local Proxy Credential Disclosure	Medium	SecurityFocus, October 1, 2004
Real Estate Management Software Real Estate Management Software 1.0	A vulnerability exists in the 'site.xml' configuration file, which could let a remote malicious user obtain sensitive information. Update available at: http://real-estate-management-software.org/realestate-management-tool-code.zip We are not aware of any exploits for this vulnerability.	Real Estate Management Information Disclosure	Medium	SecurityFocus, October 1, 2004
Real Networks RealPlayer 8, 10, RealOne Player v1 & v2, Helix Player 1.x, RealPlayer Enterprise	Multiple vulnerabilities exist: a vulnerability exists due to an error when running local RM files, which could let a malicious user execute arbitrary code; a vulnerability exists when handling malformed calls, which could let a malicious user execute arbitrary code; and an unspecified error exists that allows malicious websites and media files to delete arbitrary local files. Updates available at: http://www.service.real.com/help/faq/security/040928_player/EN/ Vulnerability has appeared in the press and other public media. Proofs of Concept exploits have been published.	RealOne Player / RealPlayer / Helix Player Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA12672, September 29, 2004
Recruitment Agency Software Recruitment Agency Software 1.0	A vulnerability exists in the 'site.xml' configuration file, which could let a remote malicious user obtain sensitive information. Update available at: http://www.recruitment-agency-software.com/recruitment-agency-software-download.php We are not aware of any exploits for this vulnerability.	Online Recruitment Agency Information Disclosure	Medium	SecurityFocus, October 1, 2004
silent-storm.co.uk Silent-Storm Portal 2.1	Multiple vulnerabilities exist: a vulnerability exists in 'home.php' and 'profile.php' due to insufficient validation of user-supplied input, which could let a remote malicious user obtain administrative privileges; and a vulnerability exists in 'index.php' due to insufficient sanitization of the 'module' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Proofs of Concept exploit scripts have been published.	Silent Storm Portal Multiple Input Validation	High	CHT Security Research, September 30, 2004
sy9.org Serendipity 0.7 beta1 & prior	Several vulnerabilities exist: a vulnerability exists in 'exit.php' and 'comment.php' due to insufficient sanitization of input passed to the 'entry_id' parameter, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability exists in 'comment.php' due to insufficient sanitization of input passed to the email and username fields, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at:	Serendipity Multiple Input Validation	High	Secunia Advisory, SA12673, September 28, 2004

	http://prdownloads.sourceforge.net/php-blog/serendipity-0.7-beta3.tar.gz?download Proofs of Concept exploits have been published.			
Symantec ON Command CCM 5.0-5.4	A vulnerability exists due to a design error that provides a number of default usernames and passwords, which could let a remote malicious user obtain sensitive information **Patches available at: http://www.symantec.com/techsupp** There is no exploit code required.	ON Command Default Usernames & Passwords	Medium	Bugtraq, September 20, 2004 **Bugtraq, September 29, 2004**
Vignette Corporation Application Portal	A vulnerability exists because the included diagnostic utility by default is accessible to anyone, which could let a remote malicious user obtain sensitive information. Workarounds available at: http://www.vignette.com/ There is no exploit code required.	Vignette Application Portal Remote Information Disclosure	Medium	@stake, Inc. Security Advisory, September 28, 2004
WordPress WordPress 1.2	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient verification of user-supplied input passed to certain parameters in various scripts, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Wordpress Multiple Cross-Site Scripting	High	Bugtraq, September 27, 2004

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Exploit (Reverse Chronological Order)	Exploit Name	Workaround or Patch Available	Script Description
October 4, 2004	6A00615BFM.html MS_SQLDenialOfServicePOC.c MSsqlDenialOfServicePOC.c	Yes	Proofs of Concept exploit scripts for the Microsoft SQL Server Remote Denial of Service vulnerability.
October 4, 2004	iceexec.zip	Yes	A Proof of Concept exploit for the Icecast Server HTTP Header Buffer Overflow vulnerability.
October 1, 2004	serendipityPoC.txt	Yes	Proof of Concept exploit for Serendipity 0.7-beta1 and below SQL injection exploit.
October 1, 2004	cutter-1.02.tgz	N/A	Cutter allows network administrators to close TCP/IP connections running over a Linux/IPtables firewall.
October 1, 2004	hotspotter-0.4.tar.gz	N/A	Hotspotter is a utility that passively monitors the network for probe request frames to identify the preferred networks of Windows XP clients, and will compare it to a supplied list of common hotspot network names.
October 1, 2004	yahooPOPS.txt	No	Exploit for the remote buffer overflows in both the POP3 and SMTP services of the YahooPOPs application.
October 1, 2004	mssql.7.0.dos.c	No	Exploit for the Mssql 7.0 remote Denial of Service buffer vulnerability. Affects Mssql 7.0 Service Pack sp0, sp1, sp2, and sp3.
October 1, 2004	chatmanx.zip chatmanxMutlipleDoSPOC.zip	No	Remote Denial of Service exploit for the memory allocation flaw in Chatman versions 1.5.1 RC1 and below.
October 1, 2004	phpPOC.txt	Yes	PHP Proof of Concept exploit that makes use of an arbitrary file upload flaw in PHP versions below 4.3.9 and 5.0.2.
October 1, 2004	alexPHP.txt	Yes	Proof of Concept exploit for the Alex PHP Guestbook remote file inclusion vulnerability.
October 1, 2004	VypressMessenger_BO_POC.zip	Yes	A Proof of Concept exploit for the VyPRESS Messenger Remote Buffer Overflow vulnerability.
September 30, 2004	Proof of Concept	No	Proof of Concept example for multiple vulnerabilities in Silent-Storm Portal. The issues result from insufficient sanitization of user-supplied data.
September 30, 2004	Proof of Concept	Yes	Proof of Concept exploits for multiple vulnerabilities in W-Agora 4.1.6a.
September 30, 2004	n-du.tgz	N/A	A Unix backdoor which does not have any open ports. It waits for a special UDP or TCP packet, then opens a tcp port backdoor.
September 30, 2004	flc_exp.c	No	Proof of Concept local exploit for elevated privilege vulnerability in flc versions 1.0.4 and below.
September 30, 2004	mdaemon_rcpt.c	No	Proof of Concept remote exploit for the Denial of Service vulnerability in Mdaemon SMTP server version 6.5.1.
September 30, 2004	mdaemon_imap.c	No	Proof of Concept remote exploit for the buffer overflow vulnerability in MDaemon IMAP server version 6.5.1.
September 29, 2004	x_hpux_11_swinstall.c	Yes	Local root exploit that makes use of a buffer overflow in the Software Distributor utilities for HP-UX.
September 29, 2004	actpboom.zip	No	Proof of Concept exploit for ActivePost Standard versions 3.1 and below that makes use of a Denial of Service flaw.
September 29, 2004	x_hpux_11i_nls_ping.c	Yes	Local format string exploit for /user/sbin/ping under HP-UX.
September 29, 2004	x_hpux_11i_nls_cu.c	Yes	Local format string exploit for /usr/bin/cu under HP-UX.
September 29, 2004	ms04-028-cmd.c JpgDownloader.c	Yes	Exploits for the Microsoft Windows (Graphics Device Interface) GDI+ JPEG handler integer underflow vulnerability.

	JpegOfDeathAll.c		
September 29, 2004	and_more_sql_injection.pdf	N/A	White paper discussing SQL injection attacks from different angles.
September 29, 2004	sharexploit.c	Yes	Proof of Concept exploit for GNU sharutils versions 4.2.1 and below local format string vulnerability.
September 29, 2004	popmsgboom.zip	Yes	Denial of Service exploit for PopMessenger versions 1.60 that makes use of a flaw when handling dialog boxes in relation to illegal characters.
September 29, 2004	aspWebCalendar.txt	No	Proof of Concept exploit for aspWebCalendar and aspWebAlbum SQL injection attack vulnerability.
September 29, 2004	abzboom.zip	No	A Proof of Concept exploit for the Playlogic Alpha Black Zero Remote Denial of Service vulnerability.
September 28, 2004	Proof of Concept	Yes	Proof of Concept exploit for Serendipity Cross-Site Scripting and SQL injection vulnerabilities.
September 28, 2004	Proof of Concept	No	Proof of Concept exploit for various Wordpress Cross-Site Scripting vulnerabilities.
September 28, 2004	Proof of Concept	No	Proof of Concept exploit for the dBpowerAMP Music Converter and Audio Player remote buffer overflow vulnerabilities when processing malformed audio and playlist files.
September 27, 2004	Proof of Concept	Yes	Proof of Concept exploit for multiple vulnerabilities in MegaBBS. These issues exist due to insufficient sanitization of user-supplied data and may allow an attacker to carry out HTTP response splitting and SQL injection attacks.
September 27, 2004	NewDawn4.c NewDawn3.c NewDawn2.c NewDawn.c	No	Exploit scripts for the Multiple Vendor TCP Packet Fragmentation Handling Denial of Service vulnerability.
September 27, 2004	zinfMediaWindowsExploitDelikon.c zinfexploit.c	No	Exploit for the remote buffer overflow vulnerability in Zinf when processing malformed playlist files. Reportedly, this issue affects Zinf version 2.2.1 for Windows.
September 27, 2004	Proof of Concept	No	Proof of Concept exploit for the BroadBoard Message Board multiple SQL injection vulnerabilities. These issues are due to a failure of the application to properly sanitize user supplied URI input prior to using it in an SQL query.

[back to top]

Trends

- US-CERT is aware of exploitation of a JPEG parsing vulnerability in the Microsoft GDI+ library. By convincing a victim to view a specially crafted JPEG image with a program that uses the GDI+ library, an attacker could execute arbitrary code with the privileges of the victim. Affected programs include Microsoft Internet Explorer, Office, Outlook, Outlook Express, and Windows Explorer. An attacker could exploit this vulnerability to install malicious code which might permit access to your computer. More information about the vulnerability is available in VU#297462. Microsoft has released patches for this vulnerability in Microsoft Security Bulletin MS04-028. Microsoft also suggests reading e-mail in plain text mode to reduce the risk associated with the HTML e-mail attack vector. Note that this workaround will prevent HTML formatted email messages from displaying properly.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Zafi-B	Win32 Worm	Stable	June 2004
3	Netsky-Z	Win32 Worm	Stable	April 2004
4	Netsky-D	Win32 Worm	Stable	March 2004
5	Netsky-B	Win32 Worm	Stable	February 2004
6	Mydoom.m	Win32 Worm	Stable	July 2004
7	Mydoom.q	Win32 Worm	Stable	August 2004
8	Bagle-AA	Win32 Worm	Stable	April 2004
9	Netsky-Q	Win32 Worm	Stable	March 2004
10	Bagle-AI	Win32 Worm	New to Table	July 2004

Table Updated October 1, 2004

Viruses or Trojans Considered to be a High Level of Threat

- Bagle-AS: A new version of the Bagle worm series is spreading rapidly across the net. Bagle-AS normally arrives in e-mails with a price or joke-related (infected) attachments with exe, cpl, scr or com extensions. Subject lines are picked from one of a series of innocuous greetings such as Re: Hello, Re: Thank you! or Re: Hi. The worm spreads by harvesting e-mails. The worm tries to disable a range of security applications and contains a backdoor that enables virus writers to control infected machines (The Register, September 29, 2004).

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type

Backdoor.Rtkit.B		Trojan
Backdoor.Sdbot.AC		Trojan
BackDoor-CIP		Trojan
Bagle.AM	Bagle.AS Bagle.BB Bagle.AZ I-Worm.Bagle.as W32.Beagle.AR@mm W32/Bagle.AM@mm W32/Bagle.az@MM Win32.Bagle.AM Win32/Bagle.18883.Worm Win32/Bagle.AM.DLL.Worm Win32/Bagle.AM.Worm Win32/Bagle.AQ	Win32 Worm
Downloader.Lunii		Trojan
Lmir.rz	Trojan.PSW.Lmir.rz	Trojan: Password Stealer
PWSteal.Bancos.M		Trojan: Password Stealer
PWSteal.Focosenha		Trojan: Password Stealer
PWSteal.Ldpinch.C		Trojan: Password Stealer
PWSteal.Tarno.J		Trojan: Password Stealer
StartPage-EZ	Trj/StartPage.IL Trojan.Win32.StartPage.lg	Trojan
W32.Bagz@mm		Win32 Worm
W32.Mydoom.AC@mm		Win32 Worm
W32.Spybot.EAS		Win32 Worm
W32/Bagle-AZ	I-Worm.Bagle.as W32/Bagle.az@MM	Win32 Worm
W32/Bagz-B	I-Worm.Bagz.b W32/Bagz.b@MM	Win32 Worm
W32/Bugbear-J	W32/Bugbear.j@MM	Win32 Worm
W32/Forbot-AR	Backdoor.Win32.Wootbot.gen W32/Gaobot.worm.gen.q WORM_WOOTBOT.K	Win32 Worm
W32/Forbot-AV	Backdoor.Win32.Wootbot.k	Win32 Worm
W32/Korgo-Q		Win32 Worm
W32/Rbot-LB	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-LC	Backdoor.Win32.Rbot.gen	Win32 Worm
W32/Rbot-LD	Backdoor.Win32.Rbot.bf W32/Sdbot.worm.gen.x WORM_RBOT.MW	Win32 Worm
W32/Sdbot-PV	Backdoor.SdBot.gen	Win32 Worm
W32/Snoop-A		Win32 Worm
W32/Xbot-D	Sdbot.worm.gen	Win32 Worm
XM97/Crex-C	X97M/Crex.A X97M.Crex	MS Excel Macro Virus

[back to top]

Last updated